On p-adic Galois representations attached to the elliptic curves over $\mathbb{F}_p$[[t]](Algebraic Number Theory)

AUTHOR(S):

Fujiwara, Yasushi

数理解析研究所講究録
603巻 1987年 79-86

On p-adic Galois representations attached to the elliptic curves over $\mathbb{F}_p[[t]]$

Yasushi Fujiwara
(University of Tokyo)

藤原 靖
(東大・理)

§1. Introduction

Let $R = \mathbb{F}_p[[t]]$ and $K = \mathbb{F}_p((t))$. Let E be an elliptic curve over R whose Hasse invariant is a uniformizer of R. Then the special fiber $E_0 = E \otimes_R \mathbb{F}_p$ is supersingular and the generic fiber $E \otimes_R K$ is ordinary.

Let $\bar{K}$ denote the algebraic closure of K. As $E \otimes_R K$ is ordinary, p-power torsion of $E(\bar{K})$ is isomorphic to the group $\mathbb{Q}_p/\mathbb{Z}_p$. Considering the Galois action on p-power torsion of $E(\bar{K})$, we get a Galois representation $g : \mathrm{Gal}(K^{sep}/K) \to \mathbb{Z}_p^\times$. In this report, we shall investigate the continuous homomorphism $\rho : K^\times \to \mathbb{Z}_p^\times$ which is associated with g via reciprocity map of local class field theory. For simplicity, we suppose that $p \geq 5$. By the method of Lubin-Tate [7], we first show the following

Proposition 1. Let the situation be as above. Then there exists a canonical local $\mathbb{F}_p$-algebra automorphism u of R which preserves the continuous homomorphism ρ, i.e. $\rho(f(u(t))) = \rho(f(t))$ for any $f \in K^\times$.

Let ρ^0 denote the restriction of ρ to $R^\times$. By the above proposition, $\mathrm{Ker}\ \rho^0$ contains the group $\left\{ \frac{f(u(t))}{f(t)} \mid f \in K^\times \right\}$. Our

main result is

Theorem. The kernel of the homomorphism $\rho^0 : R^\times \to \mathbb{Z}_p^\times$ is the closure of the group $\left\{ \frac{f(u(t))}{f(t)} \mid f \in K^\times \right\}$.

We shall give a sketch of the proof of these results. For the full proof, cf. [2]. (In [2], we deal with formal groups over R which are "generic". It is easily checked that the formal group of E is generic).

We here explain the motivation of this report. Let $k = \mathbb{F}_p(\lambda)$ with $p \neq 2$, where λ is an indeterminate. Let E_λ/k be an elliptic curve defined by the equation $y^2 = x(x - 1)(x - \lambda)$. As E_λ/k is ordinary, p-power torsion of $E_\lambda(\bar{k})$ is isomorphic to $\mathbb{Q}_p/\mathbb{Z}_p$. By considering the Galois action on p-power torsion of $E_\lambda(\bar{k})$, we obtain a Galois representation

$$r : \mathrm{Gal}(k^{sep}/k) \to \mathbb{Z}_p^\times.$$

For any place w of k, denote by r_w the restriction of r to the decomposition group at w.

If the reduction of E_λ at w is not supersingular, we can completely determine the representation r_w. In the case that E_λ has ordinary reduction at w, the representation r_w is unramified and the value of the Frobenius element is the reciprocal of the unit root of the zeta function of the special fiber at w (Theorem 4.2.2 of [6]). In the case that E_λ has bad reduction at w (i.e. $w = (\lambda)$, $(\lambda - 1)$, or (λ^{-1})), the situation is as follows (cf. Lemma 4.2.1 of [6]) : At the place $w = (\lambda)$, E_λ has split or non-split multiplicative reduction according as $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$. Thus r_w is trivial if $p \equiv 1 \pmod 4$ and is quadratic unramified if $p \equiv 3 \pmod 4$. At the place $w = (\lambda - 1)$, E_λ has split multiplicative reduction, so the representation r_w is

trivial. At the place $w = (\lambda^{-1})$, E_λ has additive reduction. By an easy calculation, we see that E_λ has split multiplicative reduction over $\mathbb{F}_p(((-\lambda^{-1})^{\frac{1}{2}}))$ and that r_w is a quadratic character corresponding to the extension $\mathbb{F}_p(((-\lambda^{-1})^{\frac{1}{2}}))/\mathbb{F}_p((\lambda^{-1}))$.

As for the case that E_λ has supersingular reduction at w, although some important results are obtained (e.g. Gross [3], Igusa [5]), the situation does not seem so clear. Our point of view is to consider the continuous homomorphism $\rho_w : k_w^\times \to \mathbb{Z}_p^\times$ (k_w denotes the completion of k at w) which is associated with r_w via reciprocity map of local class field theory. If E_λ has supersingular reduction at the place w of degree 1, our results apply to the homomorphism ρ_w (cf. Igusa [4]). The author hopes that this report might shed some light on the global representation $r : \mathrm{Gal}(k^{\mathrm{sep}}/k) \to \mathbb{Z}_p^\times$.

§2. Some invariance of ρ

In this section, we do not impose any condition on a prime p and shall prove Proposition 1 in a little generalized form. For the connection with the formulation given in the previous section, we refer to the beginning of §3.

We shall use the terminologies and results of formal groups (cf. Fröhlich [1]). For any elliptic curve A, we denote by $\hat{A}$ its formal group.

To obtain local $\mathbb{F}_p$-algebra automorphisms of R which preserve ρ, we introduce the functor M whose affine algebra is non-canonically isomorphic to R. Let $\mathfrak{C}$ denote the category of complete noetherian local $\mathbb{F}_p$-algebras with residue field $\mathbb{F}_p$. Let S be any object of $\mathfrak{C}$. The pair (G, ι) consisting of a formal group G over S and an isomorphism $\iota : G \otimes_S \mathbb{F}_p \simeq \hat{E}_0$ will be

called a rigidified lifting of $\hat{E}_0$ to S. Define the equivalence relation $\sim$ of rigidified liftings of $\hat{E}_0$ to S by setting $(G, \iota) \sim (G', \iota')$ if and only if there exists an S-isomorphism $\varepsilon : G \simeq G'$ such that $\iota = \iota' \circ \varepsilon_0$, where ε_0 denotes the special fiber of ε. We define the formal moduli functor M of $\hat{E}_0$ as a covariant functor that associates to any object S of $\mathcal{C}$ the set of $\sim$-equivalence classes of rigidified liftings of $\hat{E}_0$ to S.

Lubin and Tate [7] has shown that the functor M is pro-representable and that the affine algebra P of M is non-canonically isomorphic to $R = \mathbb{F}_p[[t]]$. In other words, they constructed a formal group $\mathcal{F}/P$ such that $\mathcal{F} \otimes \mathbb{F}_p = \hat{E}_0$ with the following property: For any rigidified lifting (G, ι) of $\hat{E}_0$ to S, there corresponds a unique local $\mathbb{F}_p$-algebra homomorphism $v : P \to S$ which makes (G, ι) and $(\mathcal{F}_{P,v}\otimes S, \text{identity})$ are $\sim$-isomorphic (We denote by $\mathcal{F}_{P,v}\otimes S$ the formal group obtained from $\mathcal{F}$ by making a scalar extension v). By the assumption that the Hasse invariant of E is a uniformizer of R, the element $(\hat{E}, \text{identity})$ corresponds to an isomorphism $\lambda : P \simeq R$ (cf. Proposition 1 of [2]).

Let φ be an automorphism of $\hat{E}_0$ over $\mathbb{F}_p$. Then φ naturally acts on the functor M as follows :

$$(G, \iota) \to (G, \varphi \circ \iota).$$

Denote by $\bar{\varphi}$ the automorphism of M defined above. Then we easily have

i) $\overline{\varphi \circ \psi} = \bar{\varphi} \circ \bar{\psi} \qquad \varphi, \psi \in \mathrm{Aut}_{\mathbb{F}_p} \hat{E}_0$

ii) $\bar{\varphi} = \text{identity} \iff \varphi \in \mathbb{Z}_p^{\times}$.

Let $\bar{\varphi}^*$ be the local $\mathbb{F}_p$-algebra automorphism of P which induces the automorphism $\bar{\varphi}$ on M. As the ring $\mathrm{End}_{\mathbb{F}_p} \hat{E}_0$ is

generated over $\mathbb{Z}_p$ by the Frobenius endomorphism F, the group $\mathrm{Aut}_{\mathbb{F}_p}\hat{E}_0$ is commutative. Thus we have

$$\overline{\varphi\circ\psi}^* = \bar{\psi}^*\circ\bar{\varphi}^* = \bar{\varphi}^*\circ\bar{\psi}^*.$$

For any $\varphi \in \mathrm{Aut}_{\mathbb{F}_p}\hat{E}_0$, we denote by $\mathcal{F}_\varphi/P$ the formal group obtained from $\mathcal{F}/P$ by making a scalar extension $\bar{\varphi}^*$.

Lemma 1 (Lubin-Tate [7]). There exists a P-isomorphism $\varphi^\dagger : \mathcal{F} \to \mathcal{F}_\varphi$ such that $\varphi^\dagger \otimes \mathbb{F}_p = \varphi$.

Proof. By the definition of $\bar{\varphi}^*$, the pairs $(\mathcal{F}, \varphi)$ and $(\mathcal{F}_\varphi, \text{identity})$ are $\sim$-equivalent. Thus there exists an isomorphism $\varphi^\dagger : \mathcal{F} \to \mathcal{F}_\varphi$ such that $\varphi = (\text{identity of } \hat{E}_0)\circ(\varphi^\dagger \otimes \mathbb{F}_p)$. Q.E.D.

For $\varphi \in \mathrm{Aut}_{\mathbb{F}_p}\hat{E}_0$, define a local $\mathbb{F}_p$-algebra automorphism u_φ of R by setting $u_\varphi = \lambda\circ\bar{\varphi}^*\circ\lambda^{-1}$. Denote by E_φ/R the elliptic curve obtained from E/R by making a scalar extension u_φ. By Lemma 1 we get an R-isomorphism $\tilde{\varphi} : \hat{E} \to \hat{E}_\varphi$ such that $\tilde{\varphi} \otimes \mathbb{F}_p = \varphi$. Thus the following proposition is almost obvious.

Proposition 1. For any $\varphi \in \mathrm{Aut}_{\mathbb{F}_p}\hat{E}_0$ and $f \in K^\times$, we have

$$\rho(f(u_\varphi(t))) = \rho(f(t)).$$

Proof. Denote by $\rho_\varphi : K^\times \to \mathbb{Z}_p^\times$ the continuous homomorphism attached to E_φ. Then we have $\rho_\varphi(f(u_\varphi(t))) = \rho(f(t))$. On the other hand, since $\hat{E}$ and $\hat{E}_\varphi$ are isomorphic over R, we easily conclude that $\rho = \rho_\varphi$. Thus $\rho(f(u_\varphi(t))) = \rho(f(t))$. Q.E.D.

§3. Main result

In this section, we assume that $p \neq 2, 3$. Then the Frobenius endomorphism F of $\hat{E}_0$ satisfies the relation $F^2 + p = 0$ in $\mathrm{End}_{\mathbb{F}_p}\hat{E}_0$ and the group $\mathrm{Aut}_{\mathbb{F}_p}\hat{E}_0/\mathbb{Z}_p^\times$ is a free $\mathbb{Z}_p$-module generated by $1 - F$. For $\varphi = 1 - F$, we shall abbreviate u_φ by u.

Let U^1 denote the group of principal units $1 + tR$ of R. To prove our theorem, we shall introduce a $\mathbb{Z}_p[[T]]$-module structure on U^1. Denote $u \circ \cdots \circ u$ (p^n-times) by $u^{[n]}$. For any nonnegative integer v, define $R_v = R/t^{v+1}R$ and $E_v = E \otimes_R R_v$. Via the canonical projection, we regard $\mathrm{End}_{R_v}\hat{E}_v$ as a subring of $\mathcal{O} = \mathrm{End}_{\mathbb{F}_p}\hat{E}_0$. The next lemma enables us to reduce the study of an automorphism u of R to that of endomorphism of $\hat{E}_n$.

Lemma 2. Let n and v be nonnegative integers. Then the following conditions are equivalent.

i) $u^{[n]}(t) \equiv t \pmod{t^{v+1}}$

ii) $\mathrm{End}_{R_v}\hat{E}_v \supset \mathbb{Z}_p + p^n\mathcal{O}$.

Cf. Lemma 1 of [2].

Let $i_n = \mathrm{ord}_R\left(u^{[n]}(t) - t\right)$, where ord_R denotes the normalized additive valuation of R. By using Lemma 2, we can determine i_0 and i_1.

Lemma 3. i) $i_0 = 2$ and $i_1 = 2p + 2$.

ii) $i_n \geq (2p + 2)p^{n-1}$ for any $n \geq 1$.

Cf. Proposition 3, Lemma 2 and Proposition 4 of [2].

We regard U^1 as a $\mathbb{Z}_p[T]$-module by setting $(Tf)(t) = \frac{f(u(t))}{f(t)}$ for $f \in U^1$. Since $\left((T+1)^{p^n}-1\right)f(t) = \frac{f(u^{[n]}(t))}{f(t)}$, we have

$$\left((T+1)^{p^n}-1\right)U^1 \subset 1 + t^i{}_nR.$$

By ii) of Lemma 3 and the fact that U^1 is complete, U^1 becomes a module over $\varprojlim \mathbb{Z}_p[T]/((T+1)^{p^n}-1) = \mathbb{Z}_p[[T]]$. Let $\Lambda = \mathbb{Z}_p[[T]]$. By i) of Lemma 3, we can determine the Λ-module structure of U^1.

Proposition 2. U^1 is a free Λ-module of rank 2 generated by any elements α and β of U^1 such that $\mathrm{ord}_R(\alpha - 1) = 1$ and $\mathrm{ord}_R(\beta - 1) = 1 + p$.

Cf. Proposition 5 of [2].

From this, we can now prove our theorem. Denote by V the closure of the group $\left\{ \frac{f(u(t))}{f(t)} \mid f \in K^\times \right\}$. By Igusa [5], we have $\rho^0(R^\times) = \mathbb{Z}_p^\times$, so $\mathrm{Ker}\ \rho^0 \subset U^1$ and $\rho^0(U^1) = 1 + p\mathbb{Z}_p$. Since $1 + p\mathbb{Z}_p$ is a free $\mathbb{Z}_p$-module of rank 1, it suffices to show that the $\mathbb{Z}_p$-module U^1/V is also free of rank 1.

As $f \in K^\times$ is written in the form $f = a \times t^n \times h$ ($a \in \mathbb{F}_p^\times$, $n \in \mathbb{Z}$, $h \in U^1$), we have

$$\left\{ \frac{f(u(t))}{f(t)} \mid f \in K^\times \right\} = \left\{ \left(\frac{u(t)}{t}\right)^z \times \frac{h(u(t))}{h(t)} \mid z \in \mathbb{Z},\ h \in U^1 \right\}.$$

Thus we get

$$V = \left\{ \left(\frac{u(t)}{t}\right)^z \times \frac{h(u(t))}{h(t)} \mid z \in \mathbb{Z}_p,\ h \in U^1 \right\}.$$

Take any element β of U^1 such that $\mathrm{ord}_R(\beta - 1) = 1 + p$. As $\mathrm{ord}_R\left(\frac{u(t)}{t} - 1\right) = 1$ by i) of Lemma 3, U^1 is a free Λ-module generated by $\alpha = \frac{u(t)}{t}$ and β. Then $V = \mathbb{Z}_p\alpha + TU^1 = \Lambda\alpha + \Lambda(T\beta)$,

hence we have $U^1/V = \Lambda\beta/\Lambda(T\beta) \simeq \Lambda/T\Lambda = \mathbb{Z}_p$. Q.E.D.

References

1. A. Fröhlich, "Formal groups," Lecture Notes in Math. 74, Springer Verlag, Berlin - New York, 1968.

2. Y. Fujiwara, On Galois actions on p-power torsion points of some one-dimensional formal groups over $\mathbb{F}_p[[t]]$, To appear in J. of Algebra.

3. B. Gross, Ramifications in p-adic Lie extensions, Journées de Géometrie Algébrique de Rennes, 1978, Astérisque 65, 81~102, Soc. Math. France, Paris, 1979.

4. J. Igusa, Class number of a definite quaternion with prime discriminant, Proc. Nat. Acad. Sci. USA. 44 (1958), 312~314.

5. J. Igusa, On the algebraic theory of elliptic modular functions, J. Math. Soc. Japan 20 (1968), 96~108.

6. N. Katz, P-adic properties of modular schemes and modular curves, Lecture Notes in Math. 350, 69~190, Springer Verlag, Berlin - New York, 1973.

7. J. Lubin, J. Tate, Formal moduli for one-parameter formal Lie groups, Bull. Soc. Math. France 94 (1966), 49~59.